~~TOP SECRET~~

TICOM/D - 34

Translation of 2 Cryptanalytic Reports By OKM/4/SKL III on Allied Naval Systems from Folder entitled "RESEARCH PROGRESS 30/11/44 - 21/3/45" = TICOM DOC. 520.

I. Progress Report on D/F System, 16/3/45.

II. General Cryptanalytic Progress Report for beginning of March, 1945.

Translations of reports in the same folder have already been issued as TICOM/D 12, D/15, and D/18.

TICOM

17th Sept. 1945. No. of Pages: 11

Distribution

British

D.D.3
H.C.G.
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
C.C.R. (2)
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (2) (via Lt. Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET (via Lt. Col. Johnson)
Col. Lewis Powell, USSTAF.

TICOM

Chairman
S.A.C.
Cdr. Bacon
Lt. Col. Johnson
Major Seaman
Lt. Cdr. Manson
Capt. King
Ticom Files (4)

Additional

S.A.C. for D.D.(C.S.A.)
S.A.C. for D.S.D. 10 Admiralty
S.A.C. 1 extra.
Commander I.C. Admiralty.

OKM 4/SKL III Fm.

To: Chef 4/SKL III

PROGRESS REPORT ON TRACKING CODE "A" ((3-LETTER)) AND "B" ((4-LETTER))

3-letter part "A".

I. January 1945.

1) Material received and review of same.

The following was received during the month of January:

	1st half	2nd half	Total;
ATLANTIC	288	197	485 messages
Indian Area	53	62	115 "
			600 "

i.e 40 W/T messages more than in December 1944. Again, as in the second half of December, U.S. D/F stations transmitted approximately three times as many D@F'ings as the British stations. Traffic from WHITEHALL to MURMANSK, which had been quite lively in the first half of December, and fell off during the second half (30 as against 2 messages) remained very slight in January. Only 2 messages on this link were intercepted during the first half of the month. GIBRALTAR, which had vanished from this traffic months before, again received one message on 22nd January.

2) INDIAN AREA.

About half of the T.O.O's could be recovered. Based on this, of the 21 frequencies which occurred, 8 were completely recovered, 6 had 1 bigram recovered, and 7 remained unidentified. No material was received from the South African area. Change ((of book)) took place as usual at 0000 hours on 1/ and 16/1.

3) ATLANTIC AREA.

The AZORES and FAROES appear to enjoy the most favourable reception conditions at present, because the majority of the material received again originated from these stations. During January, the following number of German U/Boat messages were D/F'd by the enemy D/F organisation:

1st to 15th January: 24 out of 35 messages transmitted;
16th to 31st January;: 14 out of 68 "WW" signals transmitted.

Regarding the above statement, it should be taken into account that the British D/F stations in U.K. no longer transmit their D/F results, and are thus excluded from the above review.

The basic code book changed at 0000 hours on 1 and 16 January. During the year, there was again no material received from the MED.

II. February 1945.

1) Material received and review of same.

OKM 4/SKL III Fm.

To: Chef 4/SKL III

PROGRESS REPORT ON TRACKING CODE "A" ((3-LETTER)) AND "B" ((4-LETTER))

3-letter part "A".

I. January 1945.

1) Material received and review of same.

The following was received during the month of January:

	1st half	2nd half	Total:
ATLANTIC	288	197	485 messages
Indian Area	53	62	115 "
			600 "

i.e 40 W/T messages more than in December 1944. Again, as in the second half of December, U.S. D/F stations transmitted approximately three times as many D@F'ings as the British stations. Traffic from WHITEHALL to MURMANSK, which had been quite lively in the first half of December, and fell off during the second half (30 as against 2 messages) remained very slight in January. Only 2 messages on this link were intercepted during the first half of the month. GIBRALTAR, which had vanished from this traffic months before, again received one message on 22nd January.

2) INDIAN AREA.

About half of the T.O.O's could be recovered. Based on this, of the 21 frequencies which occurred, 8 were completely recovered, 6 had 1 bigram recovered, and 7 remained unidentified. No material was received from the South African area. Change ((of book)) took place as usual at 0000 hours on 1/ and 16/1.

3) ATLANTIC AREA.

The AZORES and FAROES appear to enjoy the most favourable reception conditions at present, because the majority of the material received again originated from these stations. During January, the following number of German U/Boat messages were D/F'd by the enemy D/F organisation:

1st to 15th January: 24 out of 35 messages transmitted;
16th to 31st January;: 14 out of 68 "WW" signals transmitted.

Regarding the above statement, it should be taken into account that the British D/F stations in U.K. no longer transmit their D/F results, and are thus excluded from the above review.

The basic code book changed at 0000 hours on 1 and 16 January. During the year, there was again no material received from the MED.

II. February 1945.

1) Material received and review of same.

The following was received during February:

OKM 4/SKL III Fm.

To: Chef 4/SKL III

PROGRESS REPORT ON TRACKING CODE "A" ((3-LETTER)) AND "B" ((4-LETTER))

3-letter part "A".

I. January 1945.

1) Material received and review of same.

The following was received during the month of January:

	1st half	2nd half	Total:
ATLANTIC	288	197	485 messages
Indian Area	53	62	115 "
			600 "

i.e 40 W/T messages more than in December 1944. Again, as in the second half of December, U.S. D/F stations transmitted approximately three times as many D@F'ings as the British stations. Traffic from WHITEHALL to MURMANSK, which had been quite lively in the first half of December, and fell off during the second half (30 as against 2 messages) remained very slight in January. Only 2 messages on this link were intercepted during the first half of the month. GIBRALTAR, which had vanished from this traffic months before, again received one message on 22nd January.

2) INDIAN AREA.

About half of the T.O.O's could be recovered. Based on this, of the 21 frequencies which occurred, 8 were completely recovered, 6 had 1 bigram recovered, and 7 remained unidentified. No material was received from the South African area. Change ((of book)) took place as usual at 0000 hours on 1/ and 16/1.

3) ATLANTIC AREA.

The AZORES and FAROES appear to enjoy the most favourable reception conditions at present, because the majority of the material received again originated from these stations. During January, the following number of German U/Boat messages were D/F'd by the enemy D/F organisation:

1st to 15th January: 24 out of 35 messages transmitted;
16th to 31st January;: 14 out of 68 "WW" signals transmitted.

Regarding the above statement, it should be taken into account that the British D/F stations in U.K. no longer transmit their D/F results, and are thus excluded from the above review.

The basic code book changed at 0000 hours on 1 and 16 January. During the year, there was again no material received from the MED.

II. February 1945.

1) Material received and review of same.

The following was received during February:

	1st half	2nd half	Total:
ATLANTIC	225	328	553 messages
INDIAN AREA	63	53	116 "
			669 "

i.e., 69 more W/T messages than during January. U.S. D/F stations again transmitted about three times as many D/F'ings as the British. Of U.K. to MURMANSK traffic, only one message was intercepted in each half-month.

2) INDIAN AREA.

As the same amount of material was received as in the previous month, recoveries were maintained at about the December/January level. In the first half of February 12 frequencies occurred, in the second half 10 frequencies. Of these the following were recivered:

1st half of February: 4 completely, 6 with one bigram, 2 remained unidentified;

2nd half of February: 4 completely, 3 with one bigram, 3 remained unidentified.

5517 kc/s remained the frequency most frequently D/F'd, whereas 6815 kc/s did not appear again.

The basic book changed at 0000 hours on 1/ and 16/2.

3) ATLANTIC AREA.

The following statistics give a general review of the material intercepted by the individual enemy D/F stations in January and February:

British	1st half January	2nd half January	1st half February	2nd half February
FREETOWN	8	4	14	11
AZORES	42	35	38	46
THORSHAVEN	24	26	17	48
REYKJAVIK	4	3	9	32
ASCENSION Island	-	-	4	4
ST HELENA	2	-	-	1
ODDD	-	2	-	-
U.S.				
SAN JUAN, P.R.	42	23	31	45
GUANTANAMO	11	3	21	22
CUARACAO	9	4	21	31
TORO POINT, C.Z.	22	14	17	35
BELEM ?	47	29	25	25
GEORGETOWN ?	19	16	17	42
ODBK	20	13	15	30
NSL	13	5	17	28
NWJ	4	5	-	-
NXT	26	31	53	54
NYY	23	17	31	45
CASANLANCA	-	-	1((?-))	-
DAKAR	-	-	-	2

THORSHAVEN and REYKJAVIK stood out particularly in the second half of February by the large quantity of material they transmitted. The reasons for this could not be definitely ascertained.

A number of the D/F'ings by the U.S. stations points again to the North and North Easterly direction, as can be seen from a comparison between the two Northern Waters W/T messages.

The following number of German U/Boat messages was D/F'd in February by the enemy D/F organisation:

1st to 15th February: 8 out of 57 messages;
16th to 28th February: 15 out of 49 messages.

It is noticeable that between 25/1/45 and 12/2/45 there was no D/F'ing of German U/Boats on a subsidiary frequency. It is to be assumed that this is in result of the new W/T procedure introduced on 25/1 (change in the method of giving subsidiary frequencies and fundamental frequencies).

No material was received from the MED and South African areas. Nor, in the last month, did GIBRALTAR occur as a D/F station. It must be assumed that the duties ((of GIBRALTAR)) have been handed over to D/F stations more favourably situated for reception (AZORES ?), because it is improbable that GIBRALTAR would transmit D/F results to U.K. only by cable. The AZORES have lately played a larger part in the D/F'ing of German U/Boats. Accordingly, the greater part (15) of D/F'ings during the second half of February originated from the AZORES.

The basic book was changed as usual at 0000 hours on 1/ and 16/2.

4-letter part "B"

I. January 1945.

The January material has again decreased numerically. Only 134 messages were intercepted and worked on. The majority of these were from BOMBAY D/F station. It is to be assumed that by the far the greater part of these were check D/F'ings. It is necessary to work on these messages because they form the basis for the solution of collective D/F reports.

D/F activity in U.K. directed towards Northern Waters, which was very lively in December, was very slight in January. In the Indian and South African areas D/F activity was likewise below the average of the preceding months. The January material was not sufficient for the recovery of all D/F times. Of the 2400 groups of the basic book 350 appeared, the significations of 140 of which were recovered. The change of basic book took place at 0000 hours on 1/2.

As has already been indicated at the end of the December report, Number 12 of the series of D/F basic books came into force on 1st January. Numbers 10 and 11 have therefore been discarded. Up to Number 9 the basic book groups and their meanings changed monthly. From Number 12 onwards the groups do not change any more, only their meanings.

II. February 1945.

A slight increase of material from 134 messages in January to 152 in February 1945.

From BOMBAY alone 118 separate D/F'ings were received. As appears from Appendix 1 there were no D/F messages from the South African area. Collective reports from the Indian and Northern Waters areas likewise dimished. The difficulties arising from the transfer of the monitoring stations are most likely the main reason for the decrease of material from these areas. It is to be assumed that when the transferred stations have settled down there will be an improvement in the reception of material.

Of the 2400 groups of the basic book, 380 groups occurred. 185 of these were recovered.

The basic book changed at 0000 hours on 1/3 according to plan.

/APPENDIX

APPENDIX

Review of W/T messages intercepted by the individual monitoring stations.

Link	D/F Station	Ahlbeck			Lüchow			Beelitz			Rüg.Rad.			Campo			Soest			Hjörr			Total		
		Dec.	Jan.	Feb.	Dec.	Jan.	Feb.	Dec.	Jan.	Feb.	Dec.	Jan.	Feb.	Dec.	Jan.	Feb.	Dec.	Jan.	Feb.	Dec.	Jan.	Feb.	Dec.	Jan.	Feb.
1	Col./W'hall	18	9	5	-	-	9	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	19	9	14
12	S'town/W'hall	5	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	5	5	-
22	Bomb./W'hall	7	3	7	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	7	3	9
29	W'hall/F'town	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-
500	S'town/F'town	-	-	-	-	-	-	1	2	-	-	-	-	-	-	-	-	-	-	-	-	-	1	2	-
31	Bomb./Colom.	1	5	2	37	9	-	-	-	-	73	91	116	1	-	-	-	-	-	-	-	-	112	105	118
00	Falkl./Cleeth	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	1	-
44	F'town/Pern.	4	1	1	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	1	2
47	Waioru/Broadcast	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3	-
54	? Blank/Colom.	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	6	-	-
55	W'hall/Polyar.	25	1	2	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25	1	4
61	Belc./Colom.	3	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3	2	2
65	Calc./Colom.	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-
	Colombo/ABWS	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-
	Cleethorpes/ASHM	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	1	-	-
	Recife/Freetown	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
	Madras/Colombo	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2
		71	31	20	37	9	15	1	2	-	73	91	117	1	-	-	-	1	-	1	-	-	185	134	152

CRYPTANALYTIC PROGRESS REPORT: SITUATION AS AT BEGINNING OF MARCH, 1945.

I. Cryptanalytically, the following distinction is drawn:

a) current systems, which, among other things, produce operationally valuable results in good time, and
b) those systems requiring lengthy preliminary study for a possible break-in later.

To a) belong almost exclusively off-shore and tactical systems and in the case of G.B./U.S.A., merchant vessel systems for independently routed ships and convoy stragglers.

In order to obtain operational results in good time, the present standard of coding and cyphering demands the employment of considerably more numerous staff then was the case even a year ago.

Moreover, these systems are receiving more extensive use, which means that the material has increased both in quantity and importance.

II. The following current systems belong to a):

1) G.B./U.S.A.

a) Merchant Navy Code.

2000 messages on this system are decyphered monthly and completely read; the basic book is held.

The most important operational results obtained from it are:

Times of Arrival of ATLANTIC Convoys in British and U.S. Coastal waters, as well as distribution of the ships among ports of destination. This permits far-reaching conclusions to be drawn regarding convoy time-tables.

Successes, as and when they occur, of attacks by our U/Boats as well as damage to and losses of merchant vessels at sea.

Approach points for convoys and independently routed ships (IRISH SEA to PORT SAID).

Insight into the number of ships routed independently and solution of ships' secret callsigns, which are of assistance to traffic analysis.

Weather reports from the CHANNEL, BISCAY, MED and INDIAN OCEAN.

Staff Employed.

For successful work on this system and prompt evaluation of intelligence contained, a staff of 85 - 90 is necessary (HOLLERITH personnel inclusive).

b) British Off-shore Systems.

Within the previous year, these have been considerably improved from the cypher-technique aspect. The immediate work upon ((Sofort-Bearbeitung = ? preliminary Traffic Analysis)) and decypherment of 400 to 500 messages daily is carried out at the BIGHT and GRONINGEN out-stations, where cryptanalytic parties from the W/T Recce Section are operating. The final and comprehensive work on the systems and the general direction of the cryptanalytic work of these stations, as well as the supplying and training of staff to meet increased requirements, devolves upon 4 SKL III. Experience shows this to be absolutely necessary, because knowledge drawn from other systems must be turned to account for the regular recovery of these systems, in order to achieve successful and rapid decypherment.

Most Important Operational Results.

Numbers of coastal convoys, their time tables, sailing directions and strength.

Employment of British small naval units, laying of mines, etc.

Most extensive co-operation with Admiral Commanding S-Boats during operations by ((own)) S-Boats.

Also findings concerning ATLANTIC convoys in coastal waters and weather reports from British area.

Staff Employed.

About 85 at the out-stations.
About 10 at 4 SKL III.

c) Fleet Code.

Despite the short period of validity of the code book, which is used unrecyphered, itis possible, by using increased staff, to obtain from the system findings of current operational value concerning anti-U/Boat activity and coastal convoys. About 1500 messages are decyphered monthly.

Staff Employed.

10 persons.

d) U.S.A./British Assault Code.

At present, after conclusion of landing operations in EUROPE, the system produces mainly only weather reports from the British area, and thus fertilises the other minor systems.

Staff Employed.

4 persons.

e) D/F System G.B./U.S.A.

Current reading of the D/F system has provided a good insight into the D/F organisation and D/F technique of the enemy.

It was recently proved conclusively that the enemy is D/F'ing the subsidiary frequency U/Boat traffic - if not regularly, at least extensively. This discovery led to improvements in W/T procedure.

Staff Employed

5 persons.

2) RUSSIA

There have been extensive changes in the cypher systems of Russian small naval units, so that at present only the following can be read:

a) Aircraft Recce System in the BALTIC:
b) System for passing Aircraft Recce results to submarines, as a supplement to a);
c) Aircraft Recce System in Northern Waters;
d) Recognition Signals for the air forces in Northern Waters.

For working on these systems, small cryptanalytic parties have been detached from 4 SKL III and established at FINNSNES, PILLAU and SWINEMÜNDE; their work is controlled from this end and the staff is trained by us. Additional trained staff is also supplied.

Staff Employed.

9 at the out-stations;
4 at 4 SKL III.

III. The main enemy systems, whether British, U.S. or Russian, have so improved in the last 2 years, that their recypherments are in part quite unbreakable, or can only be tackled by the employment of very numerous staff and with great difficulty.

Work on all systems recognised as unbreakable was suspended a long time ago. Work on other systems, however, which do produce certain cryptanalytic successes but which do not guarantee any operationally valuable results was only suspended a short time ago, for reasons of economy of staff.

Similarly, only those systems are worked on at present which promise operational successes within a reasonable time and, in one special case, a British system is being worked on because it is of fundamental significance for the breaking of other important British main systems.

The following systems cannot be read at present, but promise good results at a later date:

a) Russian systems for small units (minesweepers, patrol vessels, etc) which were read until late Summer 1944, and which after the change were greatly improved from the cypher technique aspect.

The recyphering system is known and has been partly solved. It is to be expected that the amount of material received will shortly increase and that the break-in will be extended to the point of readability.

Staff Employed.

12 - 15 persons, excluding HOLLERITH personnel.

b) Swedish minor systems.

7 systems occur, of which 3 promise good results. Traffic presumably contains information on Swedish, Russian and German naval forces and merchant vessels.

Staff Employed.

10 persons.

c) The British System Naval Cypher and Naval Code.

After the introduction of the stencil with daily changing key-page and 6-monthly changing basic book, this system was for some time considered unbreakable when the basic book was not known. Work on this system was, however, postponed for a long time in the hope of obtaining or capturing a copy of the basic book.

During the latter part of the Autumn, very successful experiments were carried out, proving conclusively that the system could be solved when the basic book was available. The time taken was even considerably less than what had been estimated. The Security Service Central Office (Sicherheitshauptamt), which had been assigned the task of obtaining the basic code book, stated recently that geographical conditions determined by the military situation had reduced the possibility of obtaining one, and that in future such a possibility would diminish still further.

In contrast to the diminishing prospects of getting hold of a copy of the basic book, detailed study of the Naval Cypher/Naval Code recyphering system revealed, during the last few months, certain important weaknesses in the system, and new lines of approach were recognised which point to the probability of a break-in even without having the basic book.

In contrast to the previous method of solution, where work was based exclusively on the presence of messages recognised as being on the same recypher key (schlüsselgleich), adjacent starting points on the same lines of the key are also used as a working basis in the new method. As is known, the 10,000 subtractor groups of a daily key are so interlocked that the last figures of one recypher key are repeated as the first figures of the next one. This subtractor group relationship, corresponds to a difference relationship, if one differentiates on a sliding basis. Furthermore, a method has been developed to calculate by partial differences the arithmetical descent (arithmetisches Gefälle), that is to say by the partial figure-differences of the actual groups of the basic book. For this work, about 80 - 90 persons, including HOLLERITH Staff, were necessary for working out the positive or negative proof of the accuracy of the method.

IV. Resume of Cryptanalytic staff requirements.

a) for current systems and those which offer the possibility of being read with a small time lag, approximately 155 persons;
b) for investigation of the British main systems, and therewith the study of problems of general application, approximately 85 - 90 persons.

In connection with work on the British main systems, it should also be specially noted that current study of such problems, independent of any particular operational aims, is absolutely essential to the furtherance of cryptanalytic work in general.

Work on current systems or on such systems whose problems are quite clear means a cryptanalytic stand-still. Without study of the most difficult problems, the cryptanalysts would soon find themselves with insurmountable difficulties, presented by the rapid advances of cypher technique and by changes in systems which to-day can still be read.

Trans:
J.M.E.